CLAIMS

Please amend the claims as follows:

1. (Previously presented) A method of providing varying levels of security in a data processing system, the method comprising:

receiving information from an outside source;

retrieving a first indicator form the received information that instructs the system to operate at a higher level of security;

receiving further information from said outside source;

retrieving a separate second indicator from said further information received from said outside source, the second indicator for instructing the system to operate at a lower level of security than the higher level of security instructed by the first indicator; and

preventing operation at the lower level of security until a decrease in security levels is indicated by said second indicator; while

continuing operation of said processing system.

2. (Previously presented) The method of claim 1 wherein said receiving further information comprises:

receiving an encrypted message, said encrypted message comprising a Decreased-Security-Authorization-Code to authorize said decrease in security levels.

3. (Original) The method of claim 2 wherein said Decreased-Security-Authorization-Code authorizes a decrease in encryption/decryption levels.

4. (Original) The method of claim 2 wherein said Decreased-Security-Authorization-Code authorizes a decrease in authentication level.

5. (Original) The method of claim 2 wherein said Decreased-Security-Authorization-Code authorizes a decrease in authentication level and a decrease in encryption/decryption levels.

6. (Original) The method of claim 2 wherein said encrypted message further comprises a key for use in a decryption algorithm.

7. (Original) The method of claim 6 wherein said system stores a master key to decrypt messages comprising new decryption key values and further comprising:

using said master key stored at said system to decrypt said encrypted message.

8. (Original) The method of claim 1 and further comprising:

establishing a Security-Level-Status-Indicator at said system to indicate a level of security that is being implemented by the system.

9. (Original) The method of claim 8 wherein said Security-Level-Status-Indicator indicates a level of encryption/decryption that is being implemented by the system.

10. (Original) The method of claim 8 wherein said Security-Level-Status-Indicator indicates a level of authentication that is being implemented by the system.

11. (Original) The method of claim 8 wherein said Security-Level-Status-Indicator indicates a level of authentication and a level encryption/decryption that is being implemented by the system.

12. (Presently amended) The method of claim 8 and further comprising:

configuring said Security-Level-Status-Indicator to indicate more than two security levels so as to allow said system to utilize more than two security levels.

13. (Previously presented) The method of claim 1 and further comprising:

utilizing a cable head-end as said outside source; and

utilizing a set-top box in order to retrieve the first and second indicators from the information received from the cable head-end.

14. (Original) The method of claim 2 and further comprising using a Key Management Message to convey said Decreased Security Authorization Code.

15. (Original) The method of claim 14 wherein delivery of said Key Management Message is authenticated.

16. (Original) The method of claim 14 wherein delivery of said Key Management Message is protected against a replay attack.

17. (Original) The method of claim 14 wherein delivery of said Key Management Message is authenticated and protected against a replay attack.

18. (Original) The method of claim 1 wherein a lower level of security is non-public Key mode, wherein a higher level of security is a public Key mode, the method further comprising:

continuing operation of the system in the public Key mode until an encrypted predefined message is received by the system from the outside source.

19. (Original) The method of claim 18 wherein said system stores a master key to decrypt messages comprising new decryption key values and further comprising:

using said master key stored at said system to decrypt said encrypted message.

20. (Previously presented) A method of providing a secure transition between security levels in a data processing system, the data processing system having at least a high level of security and a low level of security for operation, the method comprising:

using the system to receive information form an outside source;

operating the system at the high level of security in response to a first security message in the information from the outside source;

continuing operation of the system at the high level of security until an encrypted, second authorization message is received by the system from the outside source authorizing a switch to a different level of security, the second authorization message being separate from the first security message.

21-32. (Cancelled)